Amendments to the Specification

Please replace the existing paragraph at page 7, lines 4-7 with the following amended paragraph:

The user inputs aid to a token, generates a private hash value X(aid) within the token, and obtains a response $r=(r_0,r_1)$ using the private key ~~X(aid)~~ x for a challenge c.

Please replace the existing paragraph at page 9, lines 12-21 with the following amended paragraph:

For example, where capabilities of certificate type are used, when a private hash function X of one token leaks, unless the issuer of the capabilities notices the leak, from this point on, each time a certificate C corresponding to the token and the authentication identifier aid is issued, persons knowing the certificate C and a private key ~~X(M)~~ x corresponding to it can pass verification without using the token. However, in this case, the leaker can be traced from the private hash value X(M).

Please replace the existing paragraph at page 18, line 12 – page 19, line 3 with the following amended paragraph:

A unique value input unit 1 is supplied with a unique value d, which is a parameter required to generate a hash function X. A message input unit 2 is supplied with a message M from which to find a hash value. A function generation unique value memory unit 3 holds a function generation unique value s, which is a parameter required to generate a value generation unique value. A value generation unique value calculation unit 4 generates a value generation unique value u from the function generation unique value s stored in the function generation unique value memory unit 3 and the unique value d inputted to the unique value input unit 1. A hash value circulation unit 5 generates a hash value X(M) by applying a hash function H to the value generation unique value u generated by the value generation unique value calculation unit 4 and the message M inputted to the message input unit 2. A hash value output unit ~~6~~ outputs the hash value X(M) generated by the hash value calculation unit 5.

Please replace the existing paragraph at page 36, line 22 – page 37, line 1 with the following amended paragraph:

The challenge generation unit 20 may generate the challenge c: at random; as ~~c=h(M)~~ c=H(M) as the hash value of a message ~~m~~ M from which to generate a signature by using a hash function ~~h~~ H; as c=K by selecting cipher text K to be decoded; and by generating random number k and affording a blind effect, by the random number k, to the cipher text K to be decoded.